Bedrohungen von morgen

VERLOCKEND. *Die Netzwerkgrenzen werden aufgrund zahlreicher neuer Zugangspunkte wie Funknetze und Virtual Private Networks immer durchlässiger.*

Netzwerke und Anwendungen werden heute immer komplexer, wodurch tausende angreifbarer Schwachstellen entstehen. Bei den Bedrohungen der ersten Generation handelt es sich um Virentypen, bei denen menschliches Zutun erforderlich ist, damit sie sich verbreiten können. In der zweiten Generation der Bedrohungen herrschen aktive Würmer vor, die Systeme und Anwendungen angreifen. Bedrohungen der dritten Generation zeichnen sich durch drei Eigenschaften aus.

- Ultraschnelle Verbreitung: Schnellere Fortpflanzung ist aus Hacker-Sicht wünschenswert. Sie verhindert ein rechtzeitiges Eingreifen der Sicherheitsadministratoren und richtet deshalb größere Schäden an.
- Ausnutzung bekannter und unbekannter Sicherheitslücken: Bei

praktisch allen Angriffen in der Vergangenheit wurden bekannte Sicherheitslücken ausgenutzt. Ein wesentlicher Grund hierfür liegt darin, dass die Entdeckung neuer Schwachstellen harte Arbeit ist und die technischen Fähigkeiten des durchschnittlichen Angreifers übersteigt.

- Mehrere Angriffsvektoren: Sicherheitsbedrohungen der dritten Generation werden mehrere Angriffsvektoren führen. Besonders anfällig werden viele neue Technologien sein. Hierzu gehören Instant Messaging, die Funknetz-Infrastruktur und Voice-over-IP-basierte Systeme. Sie sind noch nicht mit weit reichenden Funktionen zur Erkennung von Bedrohungen und zum Schutz vor schädlichem Code ausgestattet.

Regelmäßige Sicherheitsaudits, bei denen Schwachstellen in Systemen und Anwendungen analysiert werden, sind ein wichtiges Mittel, um eine starke Abwehr zu gewährleisten. Die Methoden reichen von herkömmlichen Durchdringungstests bis hin zu neuen, automatisierten Diensten, die über das Web durchgeführt werden.

Die Schlüsselelemente eines gründlichen Audits sind:

- Antiviren-Software auf dem neuesten Stand zu halten
- Rechtzeitiges Patch-Management und
- die laufende Überprüfung der Sicherheitsrichtlinien.

DER AUTOR



DR. GERHARD ESCHELBECK ist Chief Technology Officer und Vice President of Engineering, Qualys, Inc.